



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,799	03/15/2002	Patrick S. Botz	POU901164US1	4349

46369 7590 08/23/2005

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER

PEARSON, DAVID J

ART UNIT PAPER NUMBER

2137

DATE MAILED: 08/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/099,799

Applicant(s)

BOTZ ET AL.

Examiner

David J. Pearson

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 March 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-79 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-79 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 March 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 20050815
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

10

1. Claims 1-79 have been examined.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 13-17, 21, 23, 26-27, 39-43, 47, 49, 52-54, 66-70, 74, 76 and 79 are rejected under 35 U.S.C. 102(e) as being anticipated by Makower et al.

For claims 1, 27, 53 and 54, Makower et al. teach an authenticated identity translation system comprising: means for establishing an authenticated user identity responsive to an identification and authentication event (note paragraph [0032]) within a domain (note paragraph [0016]) comprising an initial authentication unit and a subsequent authentication unit (note paragraph [0022]), said identification and authentication event occurring at said initial authentication unit (note paragraph [0031]), said initial authentication unit and said subsequent authentication unit employing disparate user registries with different user identities (note paragraphs [0022] and [0035]); means for generating a token representative of said identification and authentication event to be forwarded to said subsequent authentication unit (note paragraph [0031]); and means for translating the authentication user identity of said

initial authentication unit to a local user identity of said subsequent authentication unit, wherein said subsequent authentication unit initiates said translating employing said token (note paragraphs [0031] and [0035]).

For claims 13, 39 and 66, Makower et al. teach the domain comprises a trust domain, and wherein the method further comprises initially establishing said trust domain within which the authenticated identity translation is to occur (note paragraphs [0021] and [0022]).

For claims 14, 40 and 67, Makower et al. teach said initial authentication unit comprises an initial server (note paragraph [0022]), and said subsequent authentication unit comprises at least one subsequent server (note paragraph [0020]), wherein the at least one subsequent server receives a request from the initial server (note paragraph [0031]), along with said token.

For claims 15, 41 and 68, Makower et al. teach the method of claims 14, 40 and 67 wherein said method further comprises forwarding the request and the token to multiple subsequent servers (note paragraph [0036]).

For claims 16, 42 and 69, Makower et al. teach said method further comprises one of forwarding the token to the subsequent authentication unit directly from the initial authentication unit or forwarding the token from the initial authentication unit through a

user of the initial authentication unit to the subsequent authentication unit (note paragraphs [0031] and [0032]).

For claims 17, 43 and 70, Makower et al. teach the initial authentication unit and the subsequent authentication unit reside in different partitions of a multi-partition computing environment (note paragraph [0022]).

For claims 21, 47 and 74, Makower et al. teach said domain comprises a heterogeneous computing network (note FIG. 1), and wherein said initial authentication unit and said subsequent authentication unit comprise heterogeneous computing units (note paragraph [0022]).

For claims 23, 49 and 76, Makower et al. teach the generating further comprises securing the token against modification prior to said forwarding of the token to said subsequent authentication unit (note paragraph [0031]).

For claims 26, 52 and 79, Makower et al. teach said method further comprises employing a secure protocol to transfer a request and said token from said initial authentication unit to said subsequent authentication unit (note paragraph [0022]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 2-12, 18-20, 22, 24-25, 28-38, 44-46, 48, 50-51, 55-65, 71-73, 75 and 77-78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Makower et al. as applied to claims 1, 27 and 54 above, and further in view of Loisey et al.

For claims 2, 28 and 55, Makower et al. differ from the claimed invention in that they fail to specify the domain further comprises a domain controller, and wherein said method further comprises forwarding said token from said subsequent authentication unit to said domain controller, and said translating further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein said translating includes employing a global registry of said different user identities maintained by the domain controller to translate the authenticated user identity into the local user identity for the subsequent authentication unit.

Loisey et al. teach a single sign on domain system which specifies the domain further comprises a domain controller (note paragraph [0022]), and wherein said method further comprises forwarding said token from said subsequent authentication unit to said domain controller (note paragraph [0066]), and said translating further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity, wherein said translating includes employing a global registry of said different user identities maintained by the domain controller to translate

the authenticated user identity into the local user identity for the subsequent authentication unit (note paragraphs [0058] and [0059])).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the devices of Makower et al. and Loisey et al. because Loisey et al. teaches "the domain controller allows users with a single sign-on to the networked computing environment and provides system administrators of the computer services provider or of organizations in a intranet-based networked computing environment to manage security services for internal desktop users, remote dial-up users, and external e-commerce customers."

For claims 3, 29 and 56, the combination of Makower et al. and Loisey et al. teaches the method of claims 2, 28 and 55, wherein the token comprises a translation token, said translation token includes at least some of an identity of the initial authentication unit, a user identity, a method of authentication employed, and a time stamp representative of time of authentication (note paragraphs [0028] and [0031] of Makower et al.).

For claims 4, 30 and 57, the combination of Makower et al. and Loisey et al. teaches the method of claims 3, 29 and 56 wherein said generating further comprises obtaining signing value pair information from the domain controller, and signing the translation token using said signing value pair (note paragraph [0031] of Makower et al.).

For claims 5, 31 and 58, the combination of Makower et al. and Loisey et al. teaches the method of claims 4, 30 and 57 wherein said translating by the domain controller further comprises validating the translation token signature prior to said translating of the authenticated user identity to the local user identity using the global registry of different user identities (note paragraph [0034] of Makower et al.).

For claims 6, 32 and 59, the combination of Makower et al. and Loisey et al. teaches the method of claims 5, 31 and 58 wherein said signing value pair comprises a signing value and a sequence number (note paragraph [0028] of Makower et al.), and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller (note paragraph [0031] of Makower et al.), and said validating includes employing the encryption key to validate the translation token (note paragraph [0037] of Makower et al.).

For claims 7, 33 and 60, the combination of Makower et al. and Loisey et al. teaches the method of 3, 29 and 56 wherein said generating further comprises providing the translation token to the domain controller, storing the translation token by the domain controller and obtaining a token reference, said token reference comprising an index to said stored translation token of the domain controller, wherein said forwarding and said translating employ said token reference (note paragraph [0039] of Makower et al.).

For claims 8, 34 and 61, the combination of Makower et al. and Loisey et al. teaches the method of claims 7, 33 and 60 wherein said translating further comprises employing said token reference to retrieve said translation token by the domain controller, and thereafter using said translation token to find the local user identity in the global registry of different user identities (note paragraphs [0067] and [0068] of Loisey et al.).

For claims 9, 35 and 62, the combination of Makower et al and Loisey et al. teach a method of claims 2, 28 and 55 further comprising authenticating the local user identity at the subsequent authentication unit, said authentication being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain. Note paragraph [0070] of Loisey et al., which teaches the authentication of the user at the subsequent authentication units by the domain controller. Also note paragraph [0054] of Loisey et al., which teaches the domain controller uses the software Active Directory from Microsoft Corporation. Active Directory uses access control lists (at least one authentication policy) to maintain the user's permissions (return codes) for each object.

For claims 10, 36 and 63, the combination of Makower et al. and Loisey et al. teaches a method of claims 9, 35 and 62 wherein said at least one authentication policy is user dependent. Note paragraph [0054] of Loisey et al. teaches the domain controller

Art Unit: 2137

uses the software Active Directory from Microsoft Corporation, which uses access control lists (user dependent authentication policy).

For claims 11, 37 and 64, the combination of Makower et al. and Loisey et al. teaches a method of claims 2, 28 and 55 further comprising repeating said method for at least one additional subsequent authentication unit, wherein with each repeating, said subsequent authentication unit becomes said initial authentication unit and said at least one additional subsequent authentication unit becomes said subsequent authentication unit (note paragraph [0045] of Makower et al.).

The combination of Makower et al. and Loisey et al. differ from the claimed invention in that they fail to specify repeating the authentication process for logging the user into the subsequent authentication units. Makower et al. teaches the process of subsequent authentication units becoming the initial authentication unit for additional subsequent authentication units for the process of logging the user off the subsequent authentication units.

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the device of Makower et al. and Loisey et al., which used the process of forwarding authentication tokens to additional subsequent authentication units because it would be easy and convenient way to authenticate the user to all of the servers in the domain.

For claims 12, 38 and 65, the combination of Makower et al. and Loisey et al. teaches the method of claims 2, 28 and 55 wherein said generating occurs at said initial authentication unit (note paragraph [0036] of Makower et al.).

For claims 18, 44 and 71, the combination of Makower et al. and Loisey et al. teaches the method of claims 1, 27 and 54 wherein the initial authentication unit is also another subsequent authentication unit to a further initial authentication unit establishing another authenticated user identity (note paragraph [0067] of Loisey et al.).

For claims 19, 45 and 72, the combination of Makower et al. and Loisey et al. teaches the method of claims 18, 46 and 71 wherein the subsequent authentication unit comprises said further initial authentication unit (note paragraph [0067] of Loisey et al.).

For claims 20, 46 and 73, the combination of Makower et al. and Loisey et al. teaches the method of claims 1, 27 and 54 further comprising repeating said method for multiple users, employing multiple initial authentication units, each requiring access to at least one subsequent authentication unit (note paragraph [0028] of Makower et al. and paragraph [0044] of Loisey et al.).

For claims 22, 48 and 75, the combination of Makower et al. and Loisey et al. teaches the method of claims 1, 27 and 54 wherein the domain further comprises a domain controller (note paragraph [0020] of Loisey et al.), and wherein said translating

further comprises using said token to translate by the domain controller the authenticated user identity to the local user identity (note paragraph [0031] of Makower et al.), wherein the domain controller functions as a server and the initial authentication unit and subsequent authentication unit function as clients in a client/server based model (note paragraph [0059] of Loisey et al.).

For claims 24, 50, and 77, the combination of Makower et al. and Loisey et al. differs from the claimed invention in that they fail to specify that the structure of the token is programmable by the administrator of the domain.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the structure of the token be programmable by the administrator of the domain. It is well known in the art to give administrators the option to customize the security elements of a network in order to create a network that is best suited for their needs.

For claims 25, 51 and 78, the combination of Makower et al. and Loisey et al. teaches the method of claim 1, wherein the domain further comprises a domain controller (note paragraph [0020] of Loisey et al.), and wherein said method further comprises performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating (note paragraph [0040] of Makower et al.).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David J. Pearson whose telephone number is (571) 272-0711. The examiner can normally be reached on Monday - Friday, 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DP



**EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER**